

Your Ref.: 217.1005.03

Our Ref.: P198146

Japanese Translation of International Application

1. International Application No.:
PCT/US03/21592
2. Title of the Invention:
Watermarking and Fingerprinting Digital Content Using Alternative Blocks
to Embed Information
3. International Application Date:
July 9, 2003
4. Inventor(s):
Stephen WATSON
Daniel A. COLLENS
Kevin HUI
Michael A. MALCOLM
5. Applicant(s):
KALEIDESCAPE, INC.

【書類名】 国際出願翻訳文提出書

【整理番号】 198146

【提出日】 平成17年 3月 8日

【あて先】 特許庁長官殿

【出願の表示】

【国際出願番号】 PCT/US03/21592

【出願の区分】 特許

【特許出願人】

【識別番号】 505013158

【氏名又は名称】 カレイドスケイプ・インコーポレイテッド

【代理人】

【識別番号】 100086405

【弁理士】

【氏名又は名称】 河宮 治

【電話番号】 06-6949-1261

【ファクシミリ番号】 06-6949-0361

【提出物件の目録】

【物件名】 請求の範囲の翻訳文 1

【物件名】 明細書の翻訳文 1

【物件名】 図面の翻訳文 1

【物件名】 要約書の翻訳文 1

【書類名】 特許請求の範囲**【請求項 1】**

データを埋め込むデジタルコンテンツ内の位置を選択するステップと、
可能な改変がデジタルコンテンツのパケット化を保存し、さらに、各々の可能な改変がデジタルコンテンツ内に1ビット以上のデータを埋め込む、選択された位置へ作成可能な改変を選択するステップと
を含み、位置および可能な変更に、デジタルコンテンツに対する透かしを一緒に形成する、デジタルコンテンツマーキング方法。

【請求項 2】

位置を選択するステップが、データを埋め込み可能なブロックを識別するステップを含む、請求項1に記載の方法。

【請求項 3】

可能な改変を選択するステップが、改変がブロックへ適用される際に、結果的にそのブロックに対するブロック長を変化させないように、1つ以上の改変を識別するステップを含む、請求項2に記載の方法。

【請求項 4】

デジタルコンテンツが、ランレベルコードを用いて符号化され、さらに、各位置に対する可能な改変が、同一の長さのランレベルコードを用いる、請求項3に記載の方法。

【請求項 5】

ブロックに対する可能な改変が、事前に決定された以上の量ではブロックの提示を変化させない、請求項3に記載の方法。

【請求項 6】

事前に決定された量が、最大レベル変化および最大量子化スケールに関して決定される、請求項5に記載の方法。

【請求項 7】

最大レベル変化がプラスあるいはマイナス1であり、最大量子化スケールが24である、請求項6に記載の方法。

【請求項 8】

選択された位置で、可能な改変のうちのいくつかを実際に作成するステップを含んでおり、実際の改変が、デジタルコンテンツに対する、完全な、あるいは部分的なフィンガープリントを形成する、請求項1に記載の方法。

【請求項 9】

実際の改変の一部が、複数の異なるクライアント、サーバ、あるいはキャッシュ装置で作成される、請求項8に記載の方法。

【請求項 10】

デジタルコンテンツが、MPEG符号化された映画である、請求項1に記載の方法。

【請求項 11】

デジタルコンテンツに対する透かしを決定するステップであって、この透かしは、位置、およびデータを埋め込むためのこれらの位置での可能な改変を含んでいる、ステップと

その位置で、いずれの可能な改変が作成されているかを決定するステップと、
いずれの可能な改変が作成されているかを決定するステップに応答して、ビットを抽出するステップと
を含む、デジタルコンテンツ内のフィンガープリントを検出する方法。

【請求項 12】

デジタルフォーマットのデータと、
可能な改変がデジタルコンテンツのパケット化を保存しており、さらに、各々の可能な改変がデジタルコンテンツ内に1ビット以上のデータを埋め込んでいる、選択された位置のデータへの可能な改変を含む透かしと
を含むデジタルコンテンツ。

【請求項 1 3】

選択された位置が、データを埋め込み可能なブロックである、請求項 1 2 に記載のデジタルコンテンツ。

【請求項 1 4】

各々の可能な改変が、ブロックに適用される際に、そのブロックに対してブロック長の変化をもたらさない、請求項 1 3 に記載のデジタルコンテンツ。

【請求項 1 5】

デジタルコンテンツがランレベルコードを用いて符号化されており、各位置に対する可能な改変が同じ長さのランレベルコードを用いる、請求項 1 4 に記載のデジタルコンテンツ。

【請求項 1 6】

ブロックに対する可能な改変が、事前に決定された量を超えてはブロックの提示を変化させない、請求項 1 4 に記載のデジタルコンテンツ。

【請求項 1 7】

事前に決定された量が、最大レベル変化および最大量子化スケールに関して決定される、請求項 1 6 に記載のデジタルコンテンツ。

【請求項 1 8】

最大レベル変化がプラスあるいはマイナス 1 であり、最大量子化スケールが 2⁴ である、請求項 1 7 に記載のデジタルコンテンツ。

【請求項 1 9】

若干のあるいは全ての選択位置で作成された実際の改変を含む、完全な、あるいは部分的なフィンガープリントを含んでいる、請求項 1 2 に記載のデジタルコンテンツ。

【請求項 2 0】

実際の改変の一部が、複数の異なるクライアント、サーバ、あるいはキャッシュ装置で作成された、請求項 1 9 に記載のデジタルコンテンツ。

【請求項 2 1】

デジタルコンテンツが、MPEG 符号化された映画である、請求項 1 2 に記載のデジタルコンテンツ。

【請求項 2 2】

デジタルコンテンツをネットワーク内へ注入可能なネットワークインタフェースと、プロセッサと、

デジタルコンテンツを格納し、さらに、デジタルコンテンツに対する透かしを作成するプロセッサにより実行可能なインストラクションを格納するメモリ、このインストラクションは以下のステップを含む、(a) データを埋め込むために、デジタルコンテンツ内の位置を選択するステップ、および、(b) 可能な各改変がデジタルコンテンツの packets 化を保存し、さらに、各々の可能な改変がデジタルコンテンツ内に 1 ビット以上のデータを埋め込む、選択された位置へ作成する可能な改変を選択するステップ、位置および可能な変更は、デジタルコンテンツに対する透かしを形成する、デジタルコンテンツへの透かし入れが可能な装置。

【請求項 2 3】

装置がデジタルコンテンツの配布ネットワークに対する注入ポイントである、請求項 2 2 に記載の装置。

【請求項 2 4】

位置を選択するステップが、データを埋め込み可能なブロックを識別することを含んでいる、請求項 2 2 に記載の装置。

【請求項 2 5】

可能な改変を選択するステップが、改変がブロックへ適用される際に、結果的にそのブロックに対するブロック長を変化させないように、1 つ以上の改変を識別するステップを含んでいる、請求項 2 2 に記載の装置。

【請求項 2 6】

デジタルコンテンツが、ランレベルコードを用いて符号化され、さらに、各位置に対する可能な改変が、同一の長さのランレベルコードを用いる、請求項 25 に記載の装置。

【請求項 27】

ブロックに対する可能な改変が、事前に決定された以上の量ではブロックの提示を変化させない、請求項 25 に記載の装置。

【請求項 28】

事前に決定された量が、最大レベル変化および最大量子化スケールに関して決定される、請求項 27 に記載の装置。

【請求項 29】

最大レベル変化がプラスあるいはマイナス 1 であり、最大量子化スケールが 24 である、請求項 28 に記載の装置。

【請求項 30】

インストラクションが、選択された位置で、可能な各改変のうちのいくつかを実際に作成するステップを含んでおり、実際の改変が、デジタルコンテンツに対する、完全な、あるいは部分的なフィンガープリントを形成する、請求項 22 に記載の装置。

【請求項 31】

デジタルコンテンツが、MPEG 符号化された映画である、請求項 22 に記載の装置。

【請求項 32】

透かしを入れられたデジタルコンテンツを、部分的に、あるいは完全にフィンガープリントする装置であって、この透かしは、位置、デジタルコンテンツ内のこれらの位置での可能な改変を含んでおり、

デジタルコンテンツを、ネットワークへ送り、ネットワークから受け取ることが可能なネットワークインタフェースと、

プロセッサと、

デジタルコンテンツを格納し、さらに、デジタルコンテンツにフィンガープリントするプロセッサにより実行可能なインストラクションを格納するメモリとを備え、このインストラクションは、その位置での可能な改変のうちのいくつかを実際に作成するステップを含んでいる、装置。

【請求項 33】

装置が、デジタルコンテンツに対する配布ネットワーク内の注入ポイント、キャッシュ装置、あるいはエンドビューア施設である、請求項 32 に記載の装置。

【請求項 34】

デジタルコンテンツ内のフィンガープリントを検出可能な装置であって、前記装置は、プロセッサと、

デジタルコンテンツを格納し、さらに、フィンガープリントを検出するプロセッサにより実行可能なインストラクションを格納するメモリとを備え、このインストラクションは、(a) デジタルコンテンツに対する透かしを決定するステップであって、この透かしは、位置、およびデータを埋め込むこれらの位置での可能な改変を含んでいるステップと、(b) その位置で、いずれの可能な改変が作成されているかを決定するステップと、(c) いずれの可能な改変が作成されているかを決定するステップに応答して、ビットを抽出するステップとを含む、装置。

【請求項 35】

インストラクションを含む情報を格納するメモリ、このインストラクションは、デジタルコンテンツへ透かしを入れるプロセッサにより実行可能であり、このインストラクションは以下のステップを含んでいる

データを埋め込むデジタルコンテンツ内の位置を選択するステップ；

可能な各改変がデジタルコンテンツのパケット化を保存し、さらに、各々の可能な改変がデジタルコンテンツ内に 1 ビット以上のデータを埋め込む、選択された位置で作成する可能な改変を選択するステップ；

ここで、位置および可能な変更は、デジタルコンテンツに対する透かしを一緒に形

成する。

【請求項 3 6】

装置がデジタルコンテンツの配布ネットワークに対する注入ポイントである、請求項 3 5に記載のメモリ。

【請求項 3 7】

位置を選択するステップが、データを埋め込み可能なブロックを識別することを含んでいる、請求項 3 5に記載のメモリ。

【請求項 3 8】

可能な改変を選択するステップが、改変がブロックへ適用される際に、結果的にそのブロックに対するブロック長を変化させないよう、1つ以上の改変を識別するステップを含んでいる、請求項 3 5に記載のメモリ。

【請求項 3 9】

デジタルコンテンツが、ランレベルコードを用いて符号化され、さらに、各位置に対する可能な改変が、同一の長さのランレベルコードを用いる、請求項 3 8に記載のメモリ。

【請求項 4 0】

ブロックに対する可能な改変が、事前に決定された以上の量ではブロックの提示を変化させない、請求項 3 8に記載のメモリ。

【請求項 4 1】

事前に決定された量が、最大レベル変化および最大量子化スケールに関して決定される、請求項 4 0に記載のメモリ。

【請求項 4 2】

最大レベル変化がプラスあるいはマイナス 1 であり、最大量子化スケールが 2 4 である、請求項 4 1に記載のメモリ。

【請求項 4 3】

インストラクションが、選択された位置で、可能な改変のうちのいくつかを実際に作成するステップを含み、実際の改変が、デジタルコンテンツに対する、完全な、あるいは部分的なフィンガープリントを形成する、請求項 3 5に記載のメモリ。

【請求項 4 4】

デジタルコンテンツが、MPEG 符号化された映画である、請求項 3 5に記載のメモリ。

【請求項 4 5】

インストラクションを含む情報を格納するメモリであって、このインストラクションは、透かしを入れられたデジタルコンテンツを、部分的に、あるいは完全にフィンガープリントするプロセッサにより実行可能であり、この透かしは、位置、およびデジタルコンテンツ内のこれらの位置での可能な改変を含んでおり、このインストラクションは、その位置での可能な改変のうちのいくつかを実際に作成するステップを含んでいる、メモリ。

【請求項 4 6】

装置が、デジタルコンテンツに対する配布ネットワーク内の注入ポイント、キャッシュ装置、あるいはエンドビューア施設である、請求項 4 5に記載のメモリ。

【請求項 4 7】

インストラクションを含む情報を格納するメモリであって、このインストラクションは、デジタルコンテンツ内のフィンガープリントを検出するプロセッサにより実行可能であり、

デジタルコンテンツに対する透かしを決定するステップであって、この透かしは、位置、およびデータを埋め込むこれらの位置での可能な改変を含んでいるステップと、

その位置で、いずれの可能な改変が作成されているかを決定するステップと、

いずれの可能な改変が作成されているかを決定するステップに応答して、ビットを抽出するステップと

を含む、インストラクションを含む情報を格納するメモリ。

【書類名】明細書

【発明の名称】デジタルコンテンツマーケティング方法、デジタルコンテンツ内のフィンガープリントを検出する方法、デジタルコンテンツ、デジタルコンテンツに透かしを入れる装置、透かしを入れたデジタルコンテンツにフィンガープリントをほどこす装置、デジタルコンテンツ内のフィンガープリントを検出する装置、およびインストラクションを含む情報を格納するメモリ

【技術分野】

【0001】

本発明は、デジタルコンテンツの配布に関する。

【背景技術】

【0002】

例えば、映画などのメディアストリームのためのデジタルコンテンツの配布は、いくつかの問題を受ける。1つの問題は、簡単にデジタルコンテンツの正確なコピーを作成できるため、それをする権限を有しているかいないかにかかわらず、いかなる受取人もそのコンテンツを再配付可能となることである。権限なく配布される惧れがなく、デジタルコンテンツ、特にメディアストリームのためのデジタルコンテンツを配布可能となることは有利であろう。これは、デジタルコンテンツを、例えば、コンピュータネットワーク、あるいは、（例えば、要求に応じて、あるいは今後の要求を予測して、あるいは他の何かに応じて）エンドビューアへ配布するための他の技術など、通信リンクを用いて配布することが所望されるとき、特に有利であろう。

【0003】

1つの既知の解決策は、デジタルコンテンツに、コンテンツの権限のない配布者を識別可能となる「フィンガープリント」を付けることで、結果として、できるならば潜在的な権限のない配布者を思いとどまらせようとするものである。しかしながら、デジタルコンテンツのフィンガープリンティングは、以下を含むいくつかの既知の問題を受ける。（1）そのメディアストリームの提示は、オリジナルのコンテンツを改変することにより、劣化する場合があること。（2）その受取人が、フィンガープリントを改変あるいは消去することにより、改ざんしてしまうこともあること。もしくは、（3）特に、複数の権限のない再配布者が、これらの複数の受取人が利用可能な情報を用いて、フィンガープリントが改変あるいは消去されたコピーを製造するために結託している場合は、権限がないという十分な確証のある再配布者の決定は困難となること。

【0004】

他の問題は、フィンガープリントが、オリジナルのメディアストリームの配布、デコーディング、あるいは提示を妨げるかもしれないことである。特に、オリジナルのメディアストリームが、例えば、MPEG-2フォーマットなどのように、映画用の既知のフォーマットを用いて符号化されているときは、一本の映画でさえ、含まれているデータ量はかなり大きくなる場合がある。

【発明の開示】

【発明が解決しようとする課題】

【0005】

特定のフィンガープリントされたデジタルコンテンツが配布目的のためにフィンガープリントを変えられないよう、オリジナルのMPEG符号化（オリジナルのメディアストリームのパケット化を含む）ストラクチャーを保持することは、どのようなフィンガープリンティング方法にも有利であろう。特に、以下を保証することは有利となろう。（1）フィンガープリントされたデジタルコンテンツの長さが、オリジナルのデジタルコンテンツの長さと同じであること、および、（2）フィンガープリントされたデジタルコンテンツを再計算する必要もなく、さらに、フィンガープリントされたデジタルコンテンツについての多量の間状態の情報を維持する必要もなく、ネットワークコミュニケーションの技術を使用する時などのように、デジタルコンテンツの送付を中断および再開することができること。

【課題を解決するための手段】

【0006】

本発明の1つの態様は、メディアストリーム内に情報を埋め込む方法である。この方法は以下を含んでいる。(1) 情報を埋め込むために、そのメディアストリーム内部の1組の位置を選択すること、(2) それらの位置を作成するために、1組の可能な改変を選択すること、および、(3) 可能な改変のサブセットを作成すること。位置および可能な改変の組は、本明細書では「透かし」と呼ばれる場合もある。実際の改変のサブセットは、本明細書では「フィンガープリント」と呼ばれる場合もある。

【0007】

本方法は、1つは、同一メディアストリームのオリジナルバージョンであり、また1つは、同一メディアストリームの代替バージョンであるといった、同一のメディアストリームの代替バージョンが存在する1組の位置を決定する。本明細書では「オリジナルの映画」および「代替映画」(「代替映画」)と呼ぶことがあり、あるいは、メディアストリーム内の特定のブロックを「オリジナルのブロック」および「代替ブロック」(「代替ブロック」)と呼ぶこともある。1つより多い代替映画あるいは代替ブロックが、1ビットより多い情報が各位置で埋め込可能となるよう、各位置を決定することができる。したがって、こうした各位置は、1ビット以上の情報を埋め込むことができ、この埋め込まれたビットは、その位置にオリジナルの映画あるいは代替映画が選択されているか否かに対応している。

【0008】

方法の態様は、メディアストリームの配布における変化が全くないよう、改変を選択することを含んでいる。例えば、(1) そのメディアストリームを表わすデジタルコンテンツのパケット化、あるいは、(2) メディアストリームの音声部分のビデオ部分との同期化。好適な実施例では、変更のない配布は、例えば、MPEGで符号化された映画の個々のブロックなどのような、そのメディアストリームを表わすデジタルコンテンツの部分の長さに全く変更を加えることなく実行可能である。

【0009】

好適な実施例では、この方法は、そのメディアストリーム用デジタルコンテンツのMPEG-2符号化内の、1組のイントラ符号化されたブロックを決定することを含んでいる。イントラ符号化された各ブロックは、そのブロックに対するDCT係数のための1組のランレベルの符号化された値を有している。本方法は、オリジナルの組の値と少しでも違っている代替組の値があるか否か、さらに、符号化されたブロックのビット長が変わっていないかを決定する。したがって、こうした各ブロックは、埋め込まれた情報に対する位置、およびその位置に対する改変の双方を提供して、結果的に、埋め込み可能な情報値を少なくとも1ビット提供する。代替的实施例では、ブロックの代わりにマクロブロックを使用してもよい。

【0010】

この好適な実施例は、以下の選択を有することができよう、(1) 2以下の値などの、任意の個々のブロック内で変更されるランレベルの符号化された値の数；(2) $+/-1$ レベルなどの、変更される任意のランレベルの符号化された値に対する改変の量；および(3) 24以下の量子化スケールなどの、変更される任意のランレベルの符号化された値に対しても、許容される量子化量。

【0011】

好適な実施例では、本方法は、代替ブロックを選択可能なそれらのブロックを認識すること、ランダムあるいは擬似ランダム効果に対応して、各ブロックで特定の代替ブロックを選択することを含んでいる。このタイプの効果により、フィンガープリントを「取り消す」ためにランレベルを研究しようと試みるアタックに対し、フィンガープリントが抵抗することを補助可能となる。また、それは、透かしをコンテンツの空間周波数の比較的大きな範囲にわたって広げるのを補助してもよく、アタックへの抵抗を補助する一方で、視覚効果をさらに減少させる。したがって、透かしを入れられる各映画に対して、それに透

かしを入れた特定の代替映画は、代替ブロックをオリジナルのブロックに再符号化することにより、または、ブロックを代替ブロックに再符号化することにより、情報の埋め込みをリバースするようなアタックに対しても抵抗力を有している。なぜなら、アタッカーは、これらの代替ブロック、あるいはこれらのオリジナルブロックを容易には知り得ないからである。

【0012】

好適な実施例の方法は、また、メディアストリームを表わすデジタルコンテンツに対するパケット化されたデータストリーム内部のパケットの境界にまたがる位置にあるブロックを除外する。代替ブロックは、こうしたまたがるブロックを選択しないことが好ましい。なぜならこれらのブロックにアクセスすると、パケット化されたデジタルコンテンツの解析にかかわることになり、自明でない予見、およびメディアストリームを表わすデジタルコンテンツの分析をしなければならないからである。したがって、この最適化により、本発明の好適な実施例の実現が単純化される。

【0013】

本発明は映画に限定されるものではなく、例えば、アニメーションあるいは音声などの、他のデジタルコンテンツおよびメディアストリームに対しても適用可能であるのみならず、例えば、写真あるいはイラストなどの静止メディアに対しても、さらにデータベースあるいは情報の他のコレクションに対しても適用可能である。

【発明を実施するための最良の形態】

【0014】

以下の説明では、本発明の好適な実施例は、好適な処理ステップおよびデータストラクチャーに関して説明されている。本技術分野の技術者ならば、この出願の熟読の後に、本発明の実施例は、1つ以上の汎用プロセッサ、あるいは専用プロセッサ、あるいは、特定の処理ステップならびに本明細書で説明されるデータストラクチャーに適当な他の回路を用いて実行可能であり、さらに、特定の処理ステップの実行およびデータストラクチャーは、過度の実験あるいはさらなる発明を必要としないことを認めるであろう。

【0015】

語彙

次の用語は、以下で説明するように、本発明の態様に関連し、あるいは関係している。これらの用語の一般的な意味の記述は、制限を意図するものではなく、説明を意図しているに過ぎない。

【0016】

「デジタルコンテンツ」というフレーズは、エンドビューアへの提示のために、メディアストリームあるいは他の情報を表示することを意図した、デジタルフォーマットのデータを説明する。「デジタルコンテンツ」は、例えば、メッセージヘッダー情報などのパッケージング情報とは区別される。

【0017】

「メディアストリーム」というフレーズは、一連のフレームもしくはフィールドを含む映画、あるいは一連の音声を含むオーディオなど、連続した提示を意図する情報を説明する。本明細書に使用されているように、「メディアストリーム」というフレーズは、パケットを用いて連続的に送信し、コンテンツ全体が到着する前に再生を始める、音声と画像の「ストリーミングメディア」の標準的な意味より広い意味を有している。むしろ、本明細書で用いられているように、「メディアストリーム」は、連続して届けられなければならないといういかなる特定の要件も存在しない。また、本明細書で説明するように、メディアストリームは、写真あるいはイラストなどのような静止したメディアと同様に、例えば、アニメーションあるいは音声などのような、提示のための他の情報を指す場合もあるし、情報のデータベースおよび他のコレクションを指す場合もある。

【0018】

「情報をメディアストリームに埋め込む」というフレーズは、そのメディアストリームを表示し、さらに、後に検出可能な形式で埋め込まれた情報を含む、そのメディアストリ

ームのための1組のデジタルコンテンツを生成することを説明する。

【0019】

「透かし」という用語は、情報をそのデジタルコンテンツに埋め込むことができる、デジタルコンテンツのためのスキーマを説明する。本明細書で説明するように、アタッカーは、本発明により提供される透かしを容易には取り外すことができない。しかしながら、本明細書で説明するような透かしの概念は、十分に一般的であるため、アタックに対して抵抗力を持たない透かしも含み得る。本明細書で説明するように、本発明により提供される透かしは、そのメディアストリーム内部に、情報が埋め込まれる1組の位置、および情報を埋め込むことで、これらの各位置にほどこされる可能な改変の双方を含んでいる。しかしながら、本明細書で説明するような透かしの概念は、十分に一般的であるため、情報を埋め込む他の技術を用いた透かしも含み得る。

【0020】

「フィンガープリント」という用語は、少なくとも1人の指定されたデジタルコンテンツの受取人を識別し得る程度の、情報の特定の組を説明する。本明細書で説明するように、共謀した複数のアタッカーは、本発明により提供されるフィンガープリントを容易には取り除くことができず、あるいは、彼らのうちの少なくとも1人がデジタルコンテンツの権限のない配布者として検出されるのを防ぎ得ない。しかしながら、本明細書で説明するようなフィンガープリントの概念は、十分に一般的であるため、取り除きに対してそれほど抵抗力を持たず、もしくは、デジタルコンテンツの権限のない配布者を検出するような能力を提供しないフィンガープリントも含み得る。本明細書で説明するように、本発明により、提供されるフィンガープリントはメディアストリーム内部に、透かしにより識別される各位置にほどこされる特定の組の改変を含んでいる。しかしながら、本明細書で説明するようなフィンガープリントの概念は、十分に一般的であるため、情報を埋め込み、その埋め込まれた情報を検出し、さらにデジタルコンテンツの権限のない配布者を検出する、他の技術を用いるフィンガープリントを含み得る。

【0021】

「適応」という用語は、送り主がデジタルコンテンツを受取人へ届ける処理を説明する。本明細書で説明するように、送り主は、そのデジタルコンテンツのコピーを解読し、さらにそのデジタルコンテンツにより表されるメディアストリームに情報を埋め込み（したがって、そのデジタルコンテンツを部分的にフィンガープリントする）、そして、その部分的にフィンガープリントされたデジタルコンテンツを再暗号化する。送り主は、この適応されたデジタルコンテンツを受取人に送る。

【0022】

「エンドビューア」というフレーズは、メディアストリーム用のデジタルコンテンツのデコードを受け、さらにメディアストリームの提示を受けると考えられる、メディアストリームの受取人を説明する。

【0023】

「デコード」という用語は、符号化されたフォーマットのメディアストリームのデジタルコンテンツに回答して、メディアストリームの提示の形式でのデータを生成することを説明する。本明細書で説明するように、符号化されたフォーマットは、MPEG-2などの業界基準の符号化されたフォーマットを含んでいてもよい。しかしながら、本明細書で説明するようなデコードの概念は、十分に一般的であるため、メディアストリームのための他の符号化フォーマットも含み得る。

【0024】

「提示」という用語は、例えば、映画を見る（あるいは、他の感覚）ためのオーディオおよびビジュアル情報などのような、メディアストリームを見るための形式で情報を生成することを説明する。本明細書で説明するように、映画の提示は、映画のフレームあるいはフィールドのビジュアルディスプレイのみならず、その映画に関連付けられたサウンドトラックのオーディオ提示も含み得る。しかしながら、本明細書で説明するような提示の概念は、十分に一般的であるため、オーディオ、ビジュアル、あるいはその他を含む、エ

ンドビューアが受け取る情報の生成のための、他の様々な形式を含み得る。

【0025】

「オリジナルの映画」および「代替映画」というフレーズは、1つは、本発明の態様を用いるシステムへ導入されるそのメディアストリームのオリジナルバージョンであり、そして、他の1つは、オリジナルの映画に応じて生成された、同一メディアストリームの代替バージョンであるといった、同一メディアストリームの代替バージョンを説明する。同様に、「オリジナルブロック」および「代替ブロック」というフレーズは、オリジナルの映画あるいは代替映画内の、同一の個々のブロックあるいはマクロブロックの各代替バージョンを説明する。本明細書で説明するように、オリジナルの映画と代替映画との間の違いは、代替映画が、あらゆる点において、オリジナルの映画の代わりとなり得るので、履歴的である。同様に、任意の1つのオリジナルブロックと、その関連する代替ブロックとの間の違いも、代替ブロックが、あらゆる点においてオリジナルブロックの代わりとなり得るので、履歴的である。

【0026】

「MPEG」というフレーズは、ISO/IEC（国際標準化機構／国際電気標準会議）のワーキンググループである、「動画専門家グループ（Moving Picture Experts Group）」の頭文字語である。「MPEG-1」、「MPEG-2」、および「MPEG-4」というフレーズは、それぞれ、ISO/IEC 11172、ISO/IEC 13818、およびISO/IEC 14496ドキュメント内に詳しく説明されている、メディアコンテンツを符号化する技術を指している。本発明は、MPEGでの使用に限定されるものではなく、さらに、これらの用語は、同様の性質であるか、あるいはそうでないかにかかわらず、他の符号化技術を含むように広く解釈されるべきである。

【0027】

「イントラ符号化されたブロック」という用語は、イントラ符号化されたマクロブロックの一部であるブロックを指している。イントラ符号化されたブロックおよびマクロブロックは、MPEG技術の技術分野ではよく知られた用語である。

【0028】

これらの用語および概念の拡張を含む本発明の他の、およびさらなるアプリケーションは、この出願を熟読した後には、当業者にとれば明白であろう。これらの他の、およびさらなるアプリケーションは本発明の範囲および趣旨の一部であり、またこれらは、当業者にとれば、さらなる発明あるいは過度な実験を伴うことなく、明白であろう。

【0029】

システムの要素

図1は、デジタルコンテンツに透かしを入れ、フィンガープリントをほどこすシステムのブロック図を示している。

【0030】

システム100は、ビデオ配布ネットワーク110を含んでいる。ビデオ配布ネットワーク110は、少なくとも1つの注入オリジン120、および多くのエンドビューア施設130を含んでいる。

【0031】

1. 注入オリジンからエンドビューア施設への配布

注入オリジン120は、ビデオ配布ネットワーク110外部のソースから、メディアストリーム用のデジタルコンテンツ121を受けとる。好適な実施例では、これらのソースは、例えば、映画プロダクションスタジオ、テレビスタジオ、ラジオまたはテレビのネットワークシンジケートなどのような、コンテンツプロデューサーあるいはコンテンツアグリゲータを含んでいてもよい。必要であれば、注入オリジン120は、デジタルコンテンツ121をフォーマットし、それに透かしを入れ、さらに、注入オリジン120での記憶のためにそれを暗号化する。好適な実施例では、注入オリジン120は、本明細書で説明されるように、透かしを入れ、フィンガープリントをほどこす方法を使用する。

【0032】

好適な実施例では、注入オリジン120は、少なくともインストラクションを実行することができるプロセッサ、デジタルコンテンツおよびインストラクションを格納するためのメモリ、およびネットワークインタフェースを含んでいる。

【0033】

ビデオ配布ネットワーク110は、各々が、個々に、あるいは連携して、注入オリジン120からエンドビューア施設130への、デジタルコンテンツ121を受け取り、格納し、および配布するために作用可能な、キャッシュ装置111のネットワークを含んでいる。好適な実施例では、エンドビューアからの要求は、ビデオ配布ネットワーク110に、エンドビューア施設130へデジタルコンテンツ121を配布するように促し、したがって、配布用の「プル」モデルが使用される。しかしながら、代替的实施例では、注入オリジン120あるいは他の装置は、ビデオ配布ネットワーク110に、デジタルコンテンツ121をエンドビューア施設130へ配布するよう促すことも可能であり、したがって、代替的に、「プッシュ」モデルあるいは配布用の他のモデルを用いることも可能である。

【0034】

好適な実施例では、キャッシュ装置111は、1次キャッシュ112、中間キャッシュ113、およびリーフキャッシュ114を含む、層状配布システム内に配列される。1次キャッシュ112は、デジタルコンテンツ121を注入オリジン120から直接受け取る。中間キャッシュ113は、デジタルコンテンツ121を、1次キャッシュ112、あるいは、ネットワークトポロジ的に注入オリジン120により近い、他の中間キャッシュ113から受け取る。リーフキャッシュ114は、デジタルコンテンツ121を、中間キャッシュ113から、あるいは、可能であれば1次キャッシュ112から受け取り、デジタルコンテンツ121をエンドビューア施設130へ直接配布する。

【0035】

好ましくは（すなわち、好適な実施例では）、各キャッシュ装置およびエンドビューア施設は、少なくともインストラクションを実行可能なプロセッサ、デジタルコンテンツおよびインストラクションを格納するメモリ、およびネットワークインタフェースを含んでいる。

【0036】

好適な実施例では、ビデオ配布ネットワーク110は、インターネット、あるいは、その機密保護サブセットのような冗長通信ネットワークを含んでいる。しかしながら、本発明のコンテキストでは、任意の特定の通信技術を使用するビデオ配布ネットワーク110のための、いかなる特定の要件も存在していない。代替的实施例では、デジタルコンテンツ121のコピーを、注入オリジン120から、ビデオ配布ネットワーク110を通して最終的にエンドビューア施設130へ配送可能ないかなる通信技術も適当であろう。

【0037】

好適な実施例では、ビデオ配布ネットワーク110を用いるデジタルコンテンツ121の配布は、デジタルコンテンツ121のコピーが、複数のキャッシュ装置111に記録され、および維持され、さらに、注入オリジン120からエンドビューア施設130への1つより多い経路を用いて配送し得ることを提供する。

【0038】

第1例については、デジタルコンテンツ121のコピーは、注入オリジン120から2つの異なる中間キャッシュ113（AおよびB）へ、さらに、これらの中間キャッシュ113（AおよびB）から複数のエンドビューア施設130へ配送可能である。これらの中間キャッシュ113（A）のうちの1つが、後にそのデジタルコンテンツ121のコピーを破棄する場合には、さらにエンドビューア施設130へ配送するために、他の中間キャッシュ113（B）から他のコピーを受け取ることができる。

【0039】

第2例については、デジタルコンテンツ121の異なる部分が、注入オリジン120か

ら異なる中間キャッシュ113 (AおよびB) へ配送され、次いで、これらの中間キャッシュ113 (AおよびB) から同一エンドビューア施設130へ配送されることができ。これは、例えば、ビデオ配布ネットワーク110内部の通信リンクエラー、あるいは代替的にユーザの動作などにより、デジタルコンテンツ121を注入オリジン120からエンドビューア施設130へ送る作業が中断された場合に発生し、後に再開され、完了される。

【0040】

2. 各受取人へのビデオ配布ネットワークを用いた配布
ビデオ配布ネットワーク110内の任意の送り主が、任意の受取人に対して、いつデジタルコンテンツ121を配送しても、送り主は、その受取人に対してデジタルコンテンツ121の適応を実行する。適応では、送り主は、そのデジタルコンテンツのコピーを復号化し、そのデジタルコンテンツを部分的にフィンガープリントし、さらにその部分的にフィンガープリントされたデジタルコンテンツを再暗号化することにより、情報を、そのデジタルコンテンツにより表示されるメディアストリーム内に埋め込む。

【0041】

好適な実施例では、適応は、キャッシュ装置111とエンドビューア施設130の双方を含む、あらゆる受取人に対して実行される。これは、たとえ、それらの注入オリジン120からの距離が、同一あるいは同様であっても、キャッシュ装置111間の転送も含むことになる。しかしながら、本発明の文脈では、代替的实施例において、ビデオ配布ネットワーク110の何らかの部分、デジタルコンテンツ121を復号化し、あるいは再暗号化することなく、伝送することができるよう、適応が全ての可能な受取人に対して実行されるための、いかなる特定の要件も存在していない。

【0042】

復号化と再暗号化には、異なるキーが使用されるのが好ましい。さらに、復号化と再暗号化には、異なる暗号スキームを使用することも可能である。代替的に、同一のキー、スキーム、あるいはその双方も使用可能である。

【0043】

したがって、上述したように、結果として、個々のエンドビューア施設130が、複数の受取人に対して部分的にフィンガープリントされたデジタルコンテンツ121を受け取ることは可能である。しかしながら、いずれにせよ、好適な実施例では、個々のビューアを検出するためにフィンガープリンティング方法（例えば、フィンガープリントされたデジタルコンテンツの複数の受取人の間の共謀を検出する技術を用いるなど）が提供されている。

【0044】

個々のエンドビューア施設130が、暗号化され、およびフィンガープリントされたデジタルコンテンツ121を受け取ると、その施設は、そのデジタルコンテンツ121をローカルビデオライブラリ131内へ記録する。ローカルビデオライブラリ131は、デジタルコンテンツ121を、後に1つ以上の再生要素132へ配布するために、暗号化され、およびフィンガープリントされた形式で保存する。エンドビューアによる要求に回答して、ローカルビデオライブラリ131は、デジタルコンテンツ121を、デジタルコンテンツ121が、実質的に同時に復号化され、さらに、視聴のためにエンドビューアへ提示される、1つ以上の再生要素132へ配布する。

【0045】

システム100の1つの可能な実現についてのさらなる詳細は、2003年1月31日に出願された、関連出願である米国特許出願第10/356,692号「デジタルコンテンツの並行配布およびフィンガープリンティング (Parallel Distribution and Fingerprinting of Digital Content)」(コレンズ (Collens) 他) で議論されている。

【0046】

動作方法

図2は、本発明に従う、MPEG符号化と、代替ブロック（すなわち、代替ブロック）の生成を示す。本発明は、MPEG符号化デジタルコンテンツでの使用に限定されない。MPEGの文脈での本発明の以下の議論を読んだ後は、デジタル符号化の当業者であるなら、過度の実験あるいはさらなる発明を要することなく、本発明を異なる符号化スキームおよびデータタイプに適用することができるだろう。

【0047】

図2では、デジタルコンテンツのフレーム200が、MPEG規格に従って処理される。説明の目的のために、このフレームはRGB、CMYK、あるいは何らかの他のフォーマットでのイメージフレームとして示されている。本発明はまた、他のタイプのデジタルコンテンツに適用可能である。

【0048】

フレーム自体の中のデータを処理可能である。フレーム自体の中のデータが処理される場合、そのフレームは「イントラ符号化されている」と呼ばれる。

【0049】

代替的に、そのフレームに対して予測されるデータとそのデータの相違を処理可能である。フレームデータの予測は、前のフレーム内のデータ、あるいは、前のフレームと後に続くフレームの双方のデータに基づくことが可能である。前者の場合は、このフレームは「予測」フレームと呼ばれている；後者の場合は、このフレームは「双方向」フレームと呼ばれている。

【0050】

本発明の好適な実施例は、イントラ符号化フレームのみに適用される；しかしながら、この場合にはこうした必要はない。

【0051】

フレーム200は、 16×16 画素マクロブロック210に分割される。そして、各マクロブロックは、輝度マクロブロック220およびクロミナンスマクロブロック225に分解される。図2は、 $4:2:0$ クロミナンスフォーマットを示している。このフォーマットでは、輝度マクロブロックは4つの 8×8 ブロックを含み、クロミナンスマクロブロックは2つの 8×8 ブロックを含んでいる。肉眼は、輝度変化ほどクロミナンス変化に敏感ではないので、クロミナンスデータには低解像度を用いることができる。様々なダウンサンプリング技術のいずれであれクロミナンスブロックを決定可能である。

【0052】

他のクロミナンスフォーマットでは、異なるサイズの各クロミナンスマクロブロックが使用可能である。例えば、 $4:2:2$ フォーマットでは、各クロミナンスマクロブロックは4つの 8×8 ブロック含み、さらに $4:4:4$ フォーマットでは、各クロミナンスマクロブロックは8つの 8×8 ブロックを含んでいる。

【0053】

次に、各ブロックの輝度およびクロミナンスデータが処理される。ブロックを処理するために、離散コサイン変換(DCT)がそのブロックに適用され、1組の 8×8 DCT係数230をもたらす。

【0054】

その後、DCT係数が量子化される。量子化は、全てのDCT係数を整数によりブロックに対して分割し、いかなる残余も破棄することを伴っている。この処理により、ゼロの係数の間に点在する、いくつかの非ゼロ係数がもたされる。係数が分割されるこの整数は、ブロックに対する量子化レベルである。量子化により、精度は若干の損失をもたらす；しかしながら、可能な量子化の程度に応じて、精度の損失は、エンドビューアにとり容認可能であろう（少しでも気付かれるなら）。量子化の便益は、高度なデータ圧縮が可能となることである。

【0055】

そして、ブロックに対して量子化されたデータは、パターン240などのジグザグパターンでブロックをラン(run)することにより順序付けられる。この順序付けは、ゼロ

の連続で分離されるレベルと呼ばれる、非ゼロ係数の系列をもたらす。図2では、こうした系列は、参照数字250で表現的に示されている。

【0056】

レベルおよびゼロの系列は、ランレベル符号化と呼ばれる処理を通して数の対のリストに変換される。このリスト内の数の対は、参照番号260で表される、ランレベルコードと呼ばれている。各対の第1数はランにおいてレベルに先行するゼロの数を表し、さらに、各対の第2数はレベルを表す。このようにして、例えば、AおよびBが各レベルに対する値として、レベルとゼロの系列(A 0 0 0 0 0 B 0 0)は、対(0, A) および (5, B) などに変換可能である。

【0057】

圧縮を改良するために、ランレベルコードは、ハフマンコードなどの何らかの適応型符号化スキームを通して符号化される。このタイプの符号化スキームは、結果的に、各ランレベルコードに対して長さの異なる2進コードとなる。この理由で、結果として生じるコードは、可変長コード(VLC)と呼ばれる。図2では、長さの異なるVLC270は、長さの異なるダッシュにより表されている。

【0058】

VLC270は、4つの可変長コードを表す4本のダッシュを含んでおり、これは順番に、輝度あるいはクロミナンスデータの単一の8×8画素ブロックに対する、量子化されたDCT係数のための4つのランレベルコードを表している。ブロックは、より短い、あるいはより長い長さの、より少ない、あるいはより多くのこうしたVLCにより表されることができよう。

【0059】

上で議論したように、フレームのVLCへの変換は、ダウンサンプリングおよび量子化にかかわる；その結果、VLCは正確なフレームデータを表さない。本発明は、ほとんど同一の、しかし完全には同一でない方法でフレームを表す、フレームに対するVLCの1つ以上の交互の組を決定することにより、この事実を利用する。これらのVLCの交互の組は、本発明に従う代替ブロックを形成する。VLCのオリジナルの組は、オリジナルブロックと呼ばれている。

【0060】

代替ブロックのための、若干のあるいは全てのVLCは、オリジナルブロック内のVLCとは異なる長さを有している場合もあろう。しかしながら、本発明に従えば、代替ブロックに対するVLCの全長は、オリジナルブロックに対するVLCの全長と等しくなるべきである。これは、図2において表示的に示されており、そこでは、代替ブロック280に対するVLCの全長は、オリジナルブロック290に対するVLC270の全長と等しい。

【0061】

図3は、本発明に従うパケット化の保存を示している。

【0062】

図3では、データストリーム300は、ヘッダー320内の制御データなどに加えてVLCのオリジナルブロック310を含んでいる。各ブロック内のVLCの可変数および長さは、ブロック310内の破線で表されている。

【0063】

データストリーム300は、パケット化されたデータストリーム330と同様のメディアストリームとしての提示のためにパケット化される。このパケット化されたデータストリームは、それ自身のパケットヘッダー340と、データストリーム300からの全てのデータを含むパケット350を含んでいる。パケットの境界は、図3においてパケット化されたデータストリーム330とデータストリーム300との間の縦線により示したように、データストリーム300内のいかなる場所にも発生させることが可能である。したがって、パケット境界は、ブロック310およびヘッダー320で発生可能である。

【0064】

データストリーム360は、データストリーム300内の若干のブロックの代替ブロック370を含んでいる。これらの代替ブロックは、データをデータストリーム内に埋め込むために、対応するオリジナルブロックの代わりに、データストリーム内へ挿入することができる。

【0065】

図2について議論したように、代替ブロックに対するVLCの全長は、対応するオリジナルブロックに対するVLCの全長と等しい。しかしながら、個々のVLCの数、サイズ、あるいはその両方は、総合的ブロック長が変化しない限り、オリジナルブロックのものと異なることができる。これらの変化は、ブロック370の破線により表されている。

【0066】

代替ブロックの長さが、それに対応するオリジナルブロックの長さに適合しているので、代替ブロックを伴うパケットを、オリジナルブロックを伴うパケットと置換することにより、代替ブロックを、パケット化されたデータストリーム330内へ代入可能である。

【0067】

しかしながら、代替ブロックが2つのパケットにまたがっている場合は、代替ブロックによる置換は、パケット化されたデータストリームの重要な予見および分析を必要とすることになる。したがって、本発明の好適な実施例は、データの埋め込み可能な位置から、パケットの境界にまたがるブロックを排除している。言い換えれば、代替ブロックは、パケット化されたデータストリーム内のパケットの境界にまたがるブロックを許可しないことが好ましい。

【0068】

次に、位置選択のための、およびこれらの位置に対する代替ブロックのための、好適な技術の特定の細部について議論する。デジタルコンテンツの特定のアイテムに対する可能な位置および代替ブロックの組は、そのデジタルコンテンツに対して透かしを形成する。これらの可能な代替ブロックのいくつか、あるいは全てが挿入されているコンテンツのコピーは、完全に、あるいは部分的にフィンガープリントされていると言われる。

【0069】

図4は、情報が埋め込まれるであろう1組の位置でデジタルコンテンツに透かしを入れ、フィンガープリントをほどこす方法のフロー図を示している。

【0070】

1. 透かし入れ

これらの位置でのブロック位置および代替ブロックの組は、MPEGの文脈での位置および可能な改変の組の特定の例である。概して、これらの位置でのこうした位置および可能な改変の組は、本発明に従う透かしを形成する。ステップ401およびステップ402は、この透かしの作成ステップである。これらのステップは、注入オリジン120で実行されるのが好ましい。

【0071】

ステップ401では、情報を埋め込む位置がデジタルコンテンツ内で選択される。好適な実施例では、このデジタルコンテンツは、MPEG-1、MPEG-2、あるいはMPEG-4（以下では、まとめて単にMPEGと言及する）に符号化されたデジタル映画であってもよい。以下のステップは、符号化されたデジタル映画の文脈で説明されている。しかしながら、本発明は、他のデジタルコンテンツにも等しく適用可能であり、さらに、これらのステップのアプリケーションは、さらなる発明、あるいは過度の実験を必要とはしないだろう。

【0072】

位置は、輝度あるいはクロミナンスDCT係数のいずれかの8×8ブロックであるのが好ましいが、こうした係数の16×16マクロブロックであってもよい。本発明は、完全にイントラ符号化されたマクロブロックである位置で使用可能であるが、位置は、イントラ符号化されたマクロブロックのブロックであるのが好ましい。ブロックとイントラ符号化されたマクロブロックは、MPEG符号化技術ではよく知られている。

【0073】

本発明は、例えば、ウェーブレットあるいは、輝度もしくはクロミナンス情報が、なんらかの変換されたドメイン（例えば、非MPEG符号化スキームにおける）に提示されるいかなる他の変換など、DCT以外の変換からの係数を含む他のブロックに適用可能であり、あるいは、RGBデータ、CMYKデータ、YUVデータに変換、および、より一般的に、メディアストリームの提示に役立つ情報がデジタルコンテンツで表示される、いかなる変換にも適用可能である。本技術分野の技術者ならば、この出願の熟読の後に、本発明の範囲および趣旨の中で、本質的に色空間および基礎機能のいかなる組合せも実行可能となり得て、さらに、過度の実験あるいはさらなる発明を必要としないことを認めるであろう。

【0074】

パケット化されたデジタルコンテンツの場合は、パケットの境界にまたがるブロックは、情報を埋め込むために可能な位置から排除されるのが好ましい。

【0075】

位置はまた、ブロックの代替バージョンがあり、位置に対して可能な改変を選択するよう、ステップ402で議論した評価基準を満たしているような形で選択される。したがって、ステップ401は、ステップ402に関連して起こるのが好ましい。

【0076】

ステップ402では、ブロックに対する可能な改変が選択される。デジタルコンテンツのパケット化および同期を維持するために、これらの改変は、情報が埋め込まれる位置（すなわち、ブロック）でのデジタルコンテンツの長さへ、いかなる変化も伴わないことが好ましい。

【0077】

MPEGのコンテキストでは、各ブロックは、そのブロックに対する離散コサイン変換（DCT）係数のためのランレベル符号化値の組を有している。本発明は、オリジナルの値の組と少しだけ異なっている代替の値の組があるか否か、さらにそれが符号化されたブロックのビット長を変えないかどうかを決定する。したがって、こうした各ブロックは、情報を埋め込む位置とその位置に対する改変の双方を提供し、その結果、埋め込み可能な情報の少なくとも1ビットを提供する。代替的实施例では、各マクロブロックがブロックの代わりに使用されている。

【0078】

より詳細には、MPEGでは、クロミナンスおよび輝度ブロックは、ピクセルデータ値の離散コサイン変換を表すランレベルコードに対応する可変長コード（VLC）を用いて符号化される。これらのVLCはハフマンコードであり、それはデータ圧縮の非常に効率的な方法を提供する。しかしながら、異なる各ブロックに対する結果としてのデータは、異なる長さを有している場合もある。

【0079】

したがって、情報を埋め込む位置で一定のブロック長を維持するためには、ブロックに対するVLCのいかなる変化も、正味の長ささとゼロの差にならないなければならない。これは、いくつかの方法で達成可能である。

【0080】

第1に、1つのVLCは、同一長さを有する他のVLCの代わりをすることができよう。第2に、オリジナル、および、代用されたVLCの合計の長さが等しい状態で、1つより多いVLCが、等しい数のVLCの代わりをすることもできよう。例えば、5と6の長さを有する2つのVLCは、4と7の長さを有するVLCの代わりに用いることができよう。第3に、1つ以上のVLCを追加し、あるいは削除することができよう。視覚インパクトを減少するためには、追加および削除は、1のレベルでVLCに限定されるのが好ましい。他の技術と同様、これらの3つの技術の組合せが利用可能である。

【0081】

ブロックに対する2つより多いVLCが変化する場合は、人為ストラクチャーは、たと

え非常に低いレベルの認知であれ、ビューアにより目視されるものとなろう。したがって、代替ブロックは、VLCに対する2つの変化からもたらされるブロックに限定されるのが好ましい。

【0082】

デジタルコンテンツの提示への視覚インパクトを制限するために、識別された位置のデータへの変化は、ランレベルコード内の1つのレベル値により増加し、あるいは減少するのが好ましい。加えて、MPEGは、ランレベルコードにより表されるデータの量子化に関係している。量子化スケール(QS)が24より高いなら、1のレベル変化でさえ、提示において容認できない歪みをもたらすことになる。したがって、24以下の量子化スケールを有するブロックのみが、代替ブロックの形成に使用されるのが好ましい。

【0083】

要するに、好適な実施例では、以下の評価基準は、オリジナルブロックに対する可能な改変(すなわち、代替ブロック)を識別するために使用される:

- ・ブロックは、イントラ符号化されたマクロブロックの一部である
- ・ブロックは、プラスあるいはマイナス1のレベルの値により変化可能な、1つか2つのランレベルコードを含んでいる。ランレベルにおけるその変化は、変化していないレベルに対するVLCと同一の長さを有するVLCをもたらす。(2つのランレベルコードが変化する場合、VLCの長さの合計だけが等しい必要がある)

ブロックの量子化スケールは24以下である。

【0084】

経験的に、典型的なMPEG符号化されたデジタル映画は、これらの評価基準を満たす、およそ1億の適当な位置を含んでいるのがわかっている。

【0085】

以上の評価基準の使用が好適な実施例である一方、本発明は、これらの評価基準に限定されない。したがって、本発明の代替的实施例は、イントラ符号化されていないマクロブロック内部に含まれるブロックを含む、いかなるタイプのブロックからも代替ブロックが作成可能であり、さらに、1つのブロック内の2つのVLCを変更し、追加し、あるいは削除することが可能であり、1つのレベルより大きなレベル内の変化を使用可能であり、さらに、24より大きい量子化スケールを有するブロックから代替ブロックを作成可能である。他の変化も、本発明の範囲から逸脱することなく可能である。

【0086】

図5は、代替ブロックを決定するステップ402での、ブロック内の可能な改変を識別するために使用可能な再帰的技術のフロー図を示している。非再帰的技術を含む他の異なる技術は、ステップ402の実行において、本発明から逸脱することなく、使用可能である。

【0087】

再帰的技術では、順番に、それ自体の他の例をコールする初期処理が開始される。したがって、この処理のコールされた例は、処理の他の例をコールすることなども可能である。図5では、この再帰的コールは破線として示されている。

【0088】

初期処理は、ステップ501におけるブロックに対するVLCの第1の許可された変更を作成する。VLCの変更に対して確立された、量子化レベルおよび他の任意の要件に対する評価基準を満たしている場合、VLCの変更が許可される。その後、ステップ502では、処理は、ブロックに対して変更されたVLCの長さのネット変化がゼロであるか否かを確認するようチェックする。ネット変化(再帰的処理を任意にコールすることにおける変更からの変化を含んでいる)がゼロである場合、可能な代替ブロックが見出されたことになる。可能な代替ブロックは、ステップ503で可能な代替ブロックのリストに追加される。ネット変化がゼロでない場合は、この変化はステップ504で記載(note)される。

【0089】

この処理は、そのポイントまでのネット変化をパスして、ステップ507でそれ自体の他の例を、再帰的にコールする。再帰的にコールされた処理は、ブロックに対するVLCの次の可能な変更から開始する。この次の変更とは、第1もしくは現在のVLCの他の変更、あるいは次のVLCの変更であることもあろう。

【0090】

この処理は、そのブロックの終端に達するまで、再帰的コールを続ける。処理の1つによりブロックの終端に達すると、この処理のためのフローは、ステップ505により、再帰的処理が戻るステップ506へ分流される。ここで、戻り処理をコールした処理は、ステップ508で続けられ、そのブロック内のVLCの次に許可可能な変更がなされる。この全再帰的処理は、初期処理が、そのブロックの終端に達するまで続く。

【0091】

以上の再帰的処理の理解の一助に、例を挙げることにする。この例では、2回の変化のみが、ブロックに対する3つのVLCの各々に試みられている。例を単純化するために、すべての変更が許可されていると仮定する。これらの変化は、 $A+1$ 、 $A-1$ 、 $B+1$ 、 $B-1$ 、 $C+1$ 、および $C-1$ と示されている。この例では、以下の順序のVLC変更は、正味の長さの変化がゼロであるとチェックされる： $(A+1)$ ， $(A+1, B+1)$ ， $(A+1, B+1, C+1)$ ， $(A+1, B+1, C-1)$ ， $(A+1, B-1)$ ， $(A+1, B-1, C+1)$ ， $(A+1, B-1, C-1)$ ， $(A+1, C+1)$ ， $(A+1, C-1)$ ， $(A-1)$ ， $(A-1, B+1)$ ， $(A-1, B+1, C+1)$ ， $(A-1, B+1, C-1)$ ， $(A-1, B-1)$ ， $(A-1, B-1, C+1)$ ， $(A-1, B-1, C-1)$ ， $(A-1, C+1)$ ， $(A-1, C-1)$ ， $(B+1)$ ， $(B+1, C+1)$ ， $(B+1, C-1)$ ， $(B-1)$ ， $(B-1, C+1)$ ， $(B-1, C-1)$ ， $(C+1)$ ，および $(C-1)$ 。

【0092】

図5の再帰的技術は、所与のブロックに対する、全ての可能な代替ブロックを見出すために使用可能である。しかしながら、代替的实施例では、この技術は、いったんある程度の数の可能な代替ブロックが見出されたり、あるいはいったん単一の代替ブロックが見出された場合でも停止可能である。複数の可能な代替ブロックが見出された場合は、1つ以上の可能な代替ブロックが、例えば、擬似ランダムに、可能な代替ブロックから選択可能であろう。他の変形形態も可能であり、本発明の範囲内にとどまっている。

【0093】

2. フィンガープリンティング

図4に戻って、フィンガープリンティングはステップ403で実行される。フィンガープリンティングは、情報をデジタルコンテンツに埋め込むために、選択された位置で変更のいくつかを実際に作成する処理である。MPEGの文脈では、変更は、いくつかのオリジナルブロックに代えて代替ブロックを使用することにより作成される。

【0094】

ブロックに対して1つの代替ブロックが見出された場合、その位置へ1ビットを埋め込むのにその代替ブロックが使用可能である。例えば、1組の位置および可能な変更がいったん決定されると、その位置でオリジナルブロックを使用することにより、その位置へ「0」を埋め込み可能であり、その位置で代替ブロックを使用することにより、「1」を埋め込み可能である。データを埋め込む他の構成も使用可能である。

【0095】

さらに、選択された位置で、ブロックに対して1つより多い代替ブロックが見出される場合、それらの代替ブロックは、その位置で1ビットより多くを埋め込むのに使用可能である。例えば、オリジナルブロックが「00」を表し、第1代替ブロックが「01」を表し、第2代替ブロックが「10」を表し、さらに第3代替ブロックが「11」を表すことが可能である。さらに、複数の代替ブロックを使用する他のスキームも可能である。

【0096】

ステップ403では、デジタルコンテンツ内の選択された位置のいくつかにおいて、代

替ブロックをオリジナルブロックの代わりに用いることにより、情報（すなわち、ビット）がデジタルコンテンツ内へ埋め込まれる。デジタルコンテンツの配布においては、複数の異なる点で変化を受けるのは、位置のサブセットのみであるのが好ましい。例えば、第1サブセットは1次キャッシュ112で変化を受け、第2サブセットが中間キャッシュ113で変化を受け、第3サブセットがリーフキャッシュ114で変化を受ける、などが可能である。概して、少なくともいくつかの「0」（あるいは、符号化スキームに依存する他の値）が利用可能な位置へ埋め込まれるので、各サブセット内のすべての位置が変更されるというわけではないことになる。

【0097】

3. フィンガープリント情報の抽出

フィンガープリンティングが重要であるのは、埋め込まれた情報を抽出可能であるからに他ならない。図6は、デジタルコンテンツ内のフィンガープリントから、埋め込まれた情報を抽出する方法のフロー図を示している。データは、図6に示したステップを実行可能な計算装置で抽出可能である。こうした計算装置は、少なくとも、デジタルコンテンツを格納し、さらにステップを実行するインストラクションを格納するプロセッサおよびメモリを含んでいるのが好ましい。

【0098】

ステップ601では、デジタルコンテンツの特定のアイテムに対する透かしが決定される。この透かしは、デジタルコンテンツの特定のアイテム用のそれらの位置に、1組の位置と可能な改変（例えば、代替ブロック）を含んでいる。

【0099】

透かし自体は、エンドユーザに配布されるデジタルコンテンツには含まれていないのが好ましい。したがって、デジタルコンテンツについての識別情報に基づいて、透かしは注入ポイント120から検索されるのが好ましい。こうした識別情報の例には、コンテンツのタイトル、改訂番号、シリアル番号などが含まれる。

【0100】

識別情報は、それ自体、何らかの強健な方式でデジタルコンテンツ内に埋め込まれているか、あるいはデジタルコンテンツから自明であることが好ましい。例えば、MPEG符号化された映画の場合は、識別情報は映画のタイトルであることもあり、これは、映画の内容から自明である。他の識別情報も利用可能である。

【0101】

透かしがいったん検索されると、ステップ602で、透かしにより決定される情報を埋め込む選択位置を検査可能である。位置は、透かしにより特定される可能な改変に従って、各位置のうちのいずれが改変されたかを決定するために検査される。

【0102】

次に、ステップ603では、改変（例えば、代替ブロック）が存在しているか、あるいは存在していないかの検査から、埋め込まれた情報を抽出可能である。例えば、存在している改変がデジタルの「1」を表し、存在していない改変がデジタルの「0」を表すことができる。本発明から逸脱することなく、他の符号化スキームが使用可能である。

【0103】

各々の埋め込まれたビット情報は、デジタルコンテンツ内に何度も埋め込まれるのが好ましい。これにより、いくつかの位置で改変の喪失あるいは変造があっても、埋め込まれた情報は喪失しないことになる。

【0104】

加えて、デジタルコンテンツ内の位置の順序は、既知であるがランダム（あるいは、擬似ランダム）な何らかの方式で埋め込まれた情報における、ビットの順序に関連しているのが好ましい。この埋め込み情報の混ぜ合わせは、埋め込まれた情報への権限のないアクセス、あるいは変造の防止を補助する。

【0105】

検査されるデジタルコンテンツは、故意にあるいは偶発的に改変されたこともあろう。

結果として、デジタルコンテンツ内のいかなる所与のブロックも、コンテンツの透かしからのオリジナルブロックあるいは代替ブロックのどちらとも、正確には整合しないこともある。この問題を処理するために、例えば、VLCから得られるDCT係数のベクトルスペースなど、何らかのベクトルスペース内の対応するオリジナルブロックからの各ブロックの距離が計算可能であろう。その後、オリジナルブロックあるいは代替ブロックの何らかの距離以内にあるブロックは、これらのブロックに整合するとみなすことができよう。埋め込まれたデータの各ビットが何度も埋め込まれている場合、埋め込まれたデータを計算するために、十分なビットが抽出されることになる。

【0106】

本発明の一般性

代替ブロックの生成は、デジタルコンテンツに対して使用される符号化のタイプに依存していない。一般的な意味で、本発明の透かし入れ技術およびフィンガープリントをほどこす技術は、連続の、あるいはアナログの物理処理をモデル化する、いかなるデジタルデータにも適用可能である。本発明は、MPEG-ハフマンコード化、あるいは他の完全に異なる符号化スキームを使用しているか否かに関係なく、MPEGの何らかのバージョンにより符号化された、デジタル化された音声データ、測定データ、ビデオデータ、他のマルチメディアデータなどに適用可能である。データを埋め込むために、デジタルコンテンツ内の位置を選択し、さらに、選択された位置へほどこされる可能な改変を選択するために、本発明の技術はこのデジタル化されたデータのいずれにも使用可能であり、その間ずっと、データの packets 化が保存される。

【0107】

さらには、本発明は、メディアストリームの配布以外およびデジタルコンテンツの配布以外のアプリケーションにも役立ち、十分な一般性を有している。例えば、本発明は、また、概して、データセットのセキュリティ、あるいはそれらのデータセットの受取人を識別することが所望されているアプリケーションに役立つ。

【0108】

このように、本明細書には、好適な実施例が開示されているが、本発明の概念、範囲、および趣旨内に留まりながらも、多くの変形形態が可能である。これらの変形形態は、本明細書を熟読するならば、当業者には明白になる。

【図面の簡単な説明】

【0109】

【図1】デジタルコンテンツに透かしを入れ、フィンガープリントをほどこすシステムのブロック図である。

【図2】本発明に従う、MPEG符号化と、代替ブロックの生成を示す図である。

【図3】本発明に従う、パケット化の保存を示す図である。

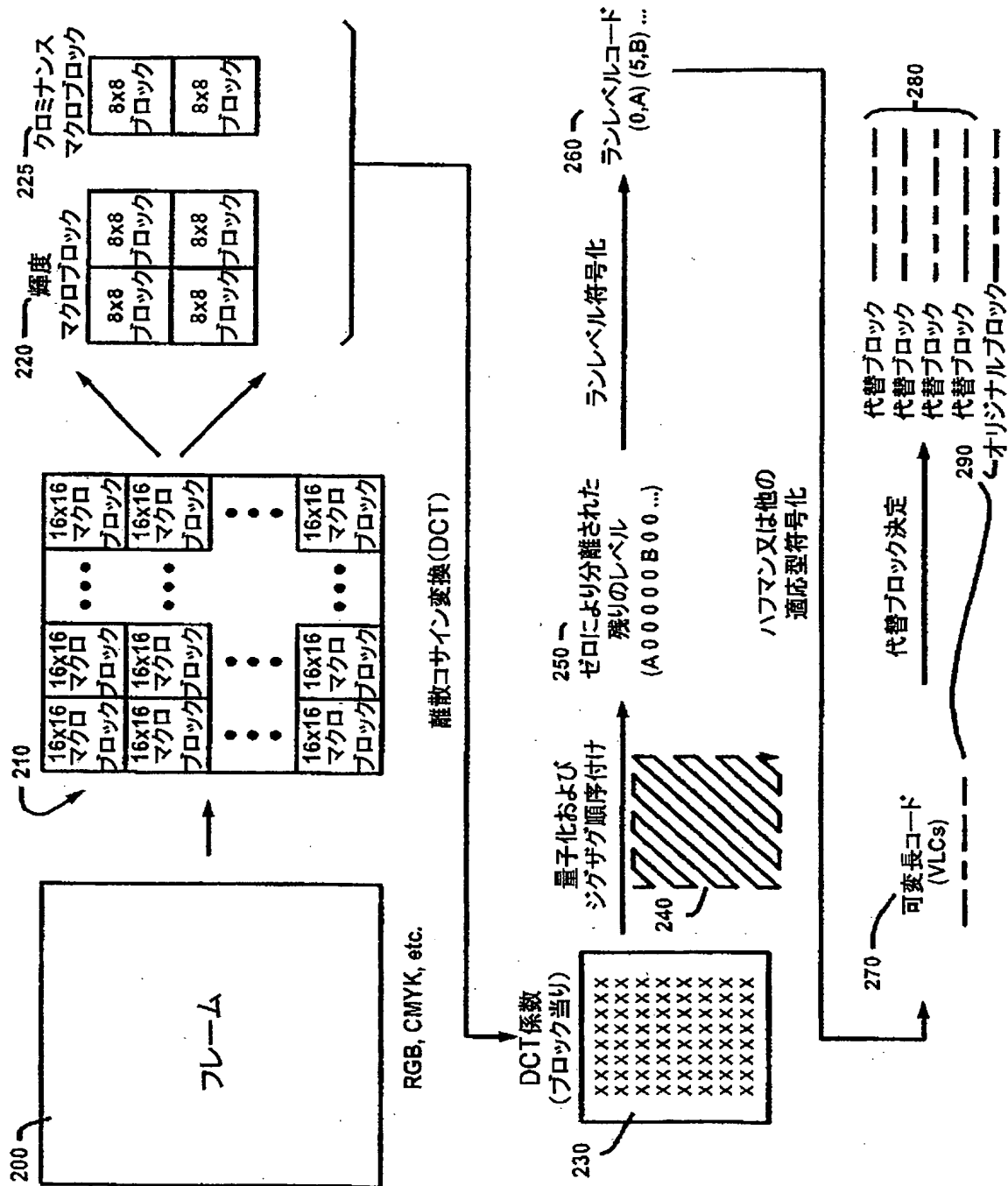
【図4】情報が埋め込まれることになる1組の位置で、デジタルコンテンツに透かしを入れ、フィンガープリントをほどこす方法のフロー図である。

【図5】本発明に従う、代替ブロックを決定するために、ブロック内の可能な改変を識別するために使用可能な再帰的技術のフロー図である。

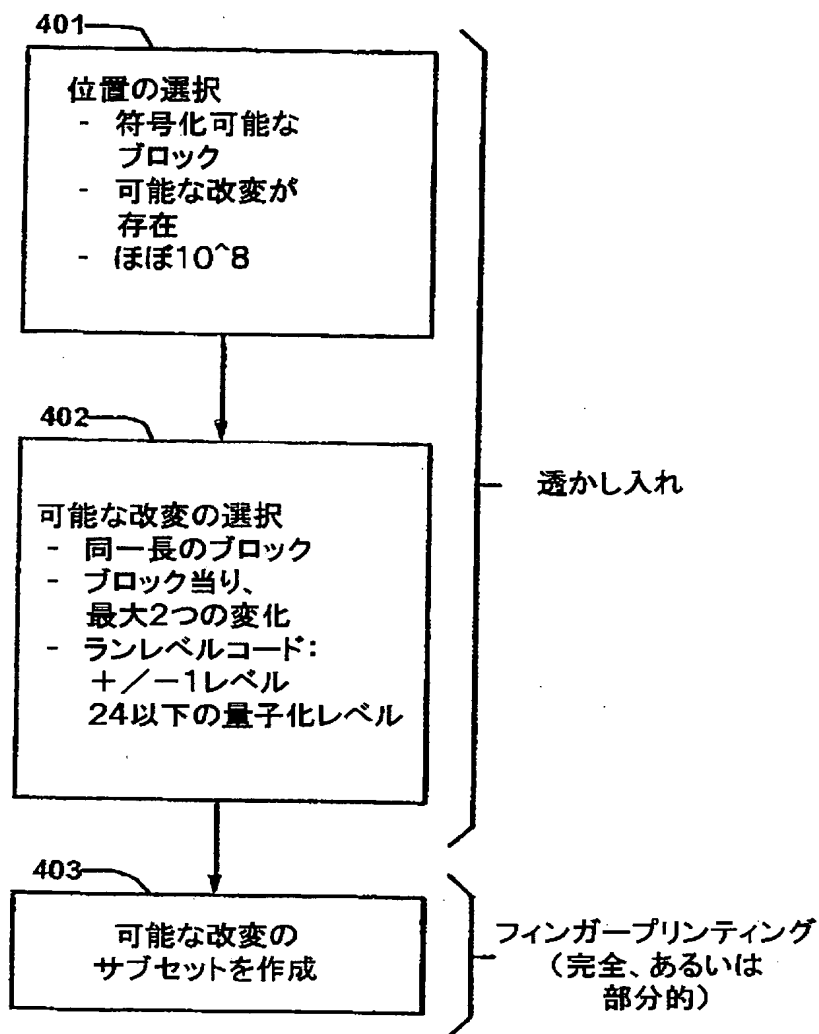
【図6】情報をデジタルコンテンツに埋め込むフィンガープリントの検出方法のフローチャートを示す図である。

【書類名】図面

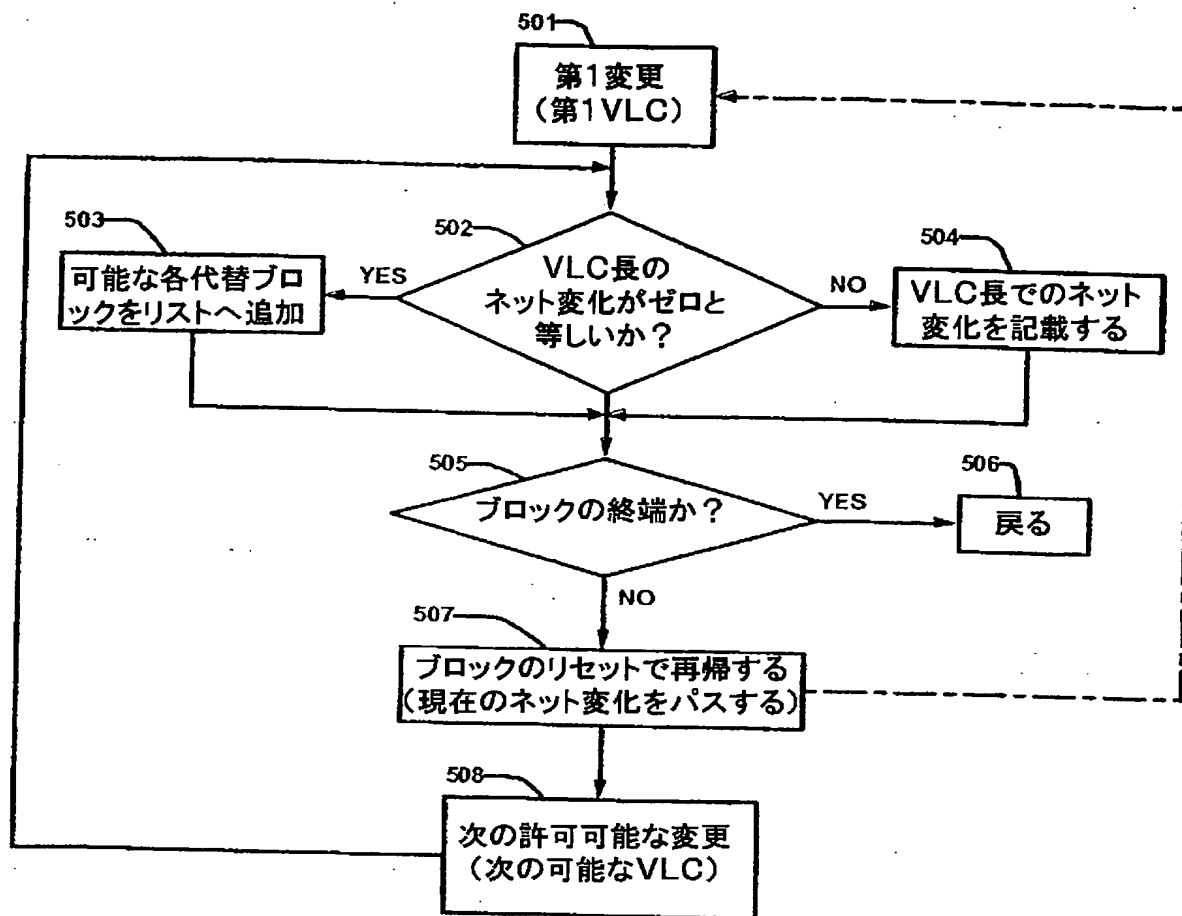
【図 2】



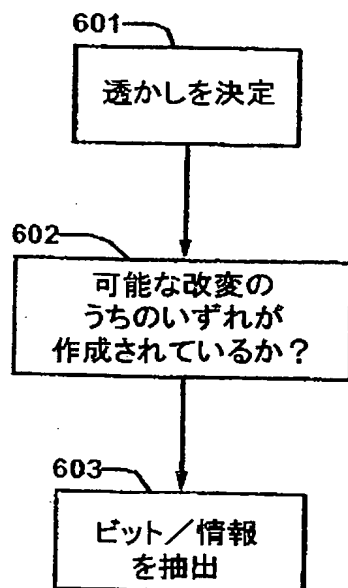
【図4】



【図5】



【図6】



【書類名】要約書

【要約】

メディアストリームを表わすデジタルコンテンツに情報を埋め込む方法。本方法は、メディアストリームを表示するそのデジタルコンテンツ内部に、情報を埋め込む1組の位置を選択すること(401)、これらの位置にほどこされる可能な1組の改変を選択すること(402)、および可能な改変のサブセットを作成すること(403)を含んでいる。位置および可能な改変の組は、本明細書では「透かし」と呼ばれる場合もある。実際の改変のサブセットは、本明細書では「フィンガープリント」と呼ばれる場合もある。本方法は、同一のメディアストリームを表わすデジタルコンテンツの代替バージョンが存在する1組の位置を決定する(601)。